# The Health Insurance Portability and Accountability Act

## Administrative Simplification

Wes Rishel
Research Director
Healthcare Industry
Research & Advisory Services
The GartnerGroup

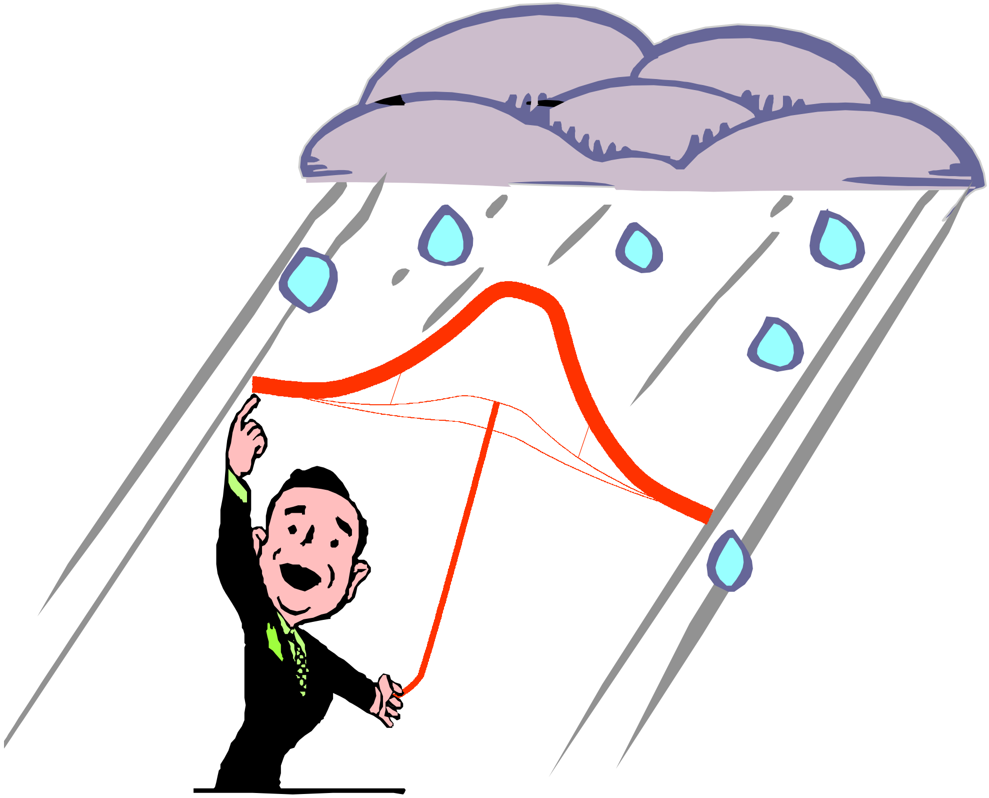
# Important Issues

**What are the HIPAA provisions that will be in the Final Rules, survive the elections and have substantial, near-term impact on clients?**

**Given the uncertainties, what can healthcare organizations do now to prepare for HIPAA?**

**How should healthcare organizations prioritize investments in HIPAA compliance?**

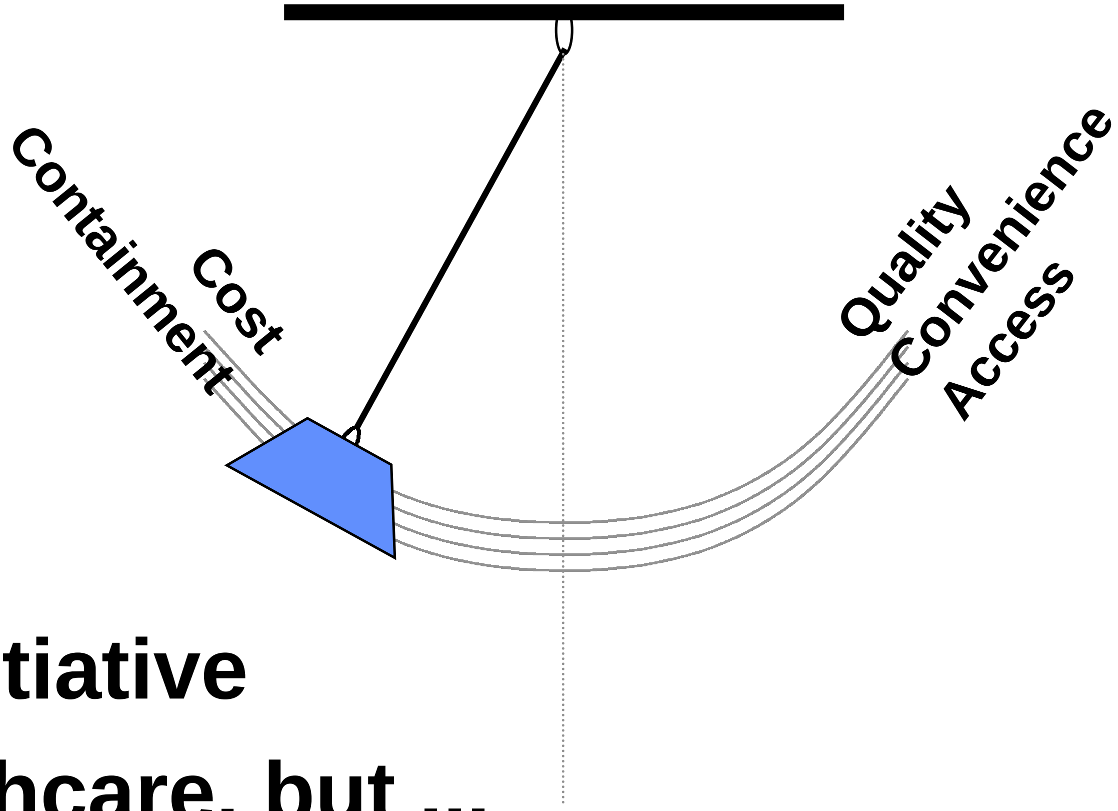
# Business Strategies



**“Hiding in the bell curve”**

**Seeking competitive advantage**

# HIPAA-AS: **Cost Driven Initiative**

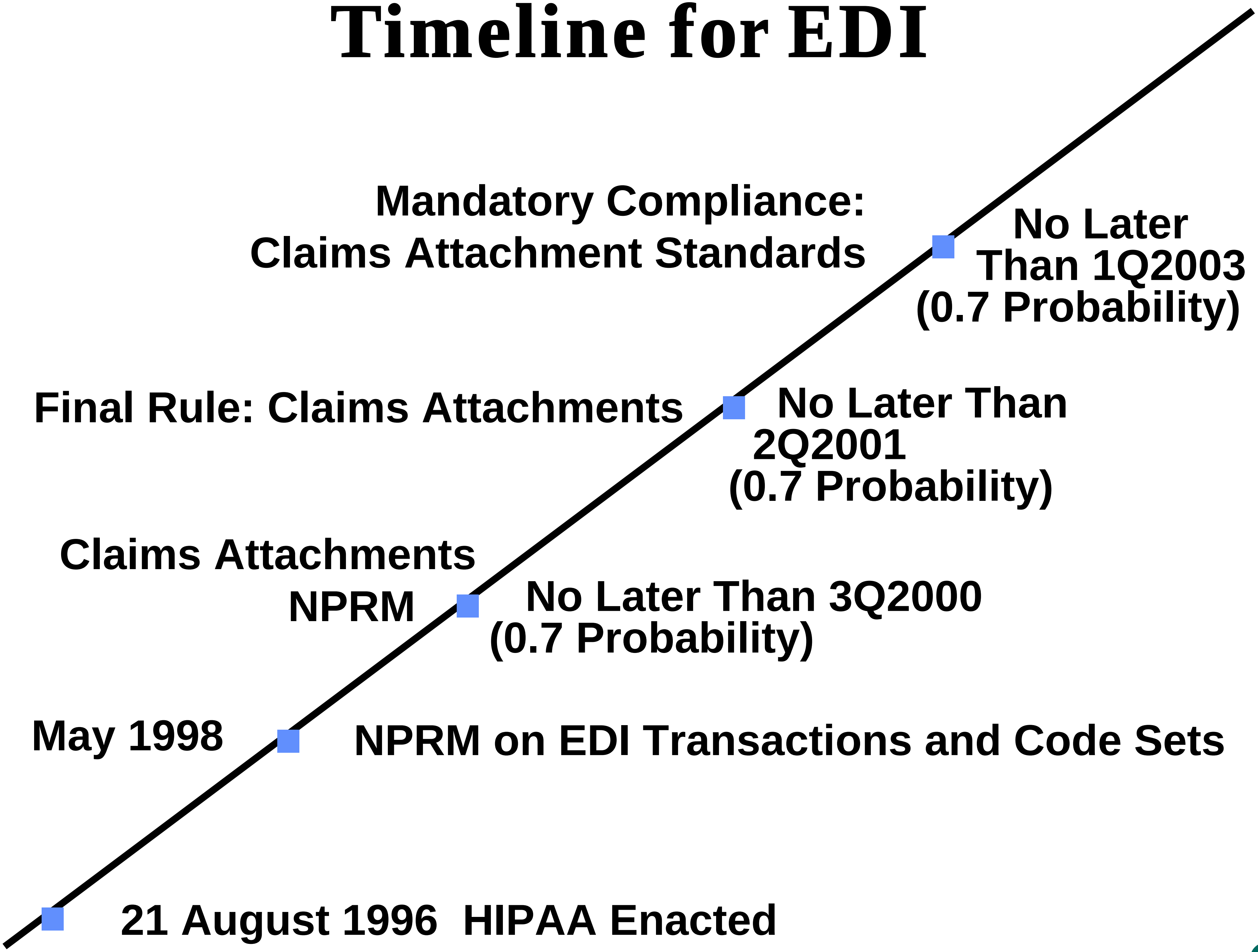


- **Cost-driven initiative**
- **Good for healthcare, but ...**
- **… Strong medicine**

# HIPAA-mandated HHS Standards

- **Electronic Transactions & Code Sets (ANS X12N & NCPDP for Rx)**
  - PLUS National Identifiers (separate standards)
    - Employers, providers, health plans
    - **Individuals?!** (ON HOLD - linked by White House to privacy legislation)
- **Security and Electronic Signature**
  - Administrative
  - Physical
  - Information storage and access
  - Information transmission
  - Electronic signatures
- **Privacy of Individually Identifiable Health Information**
  - Release requires written patient authorization (uncoerced, revocable) except for:
    - treatment, payment, healthcare operations, specific exceptions
  - Accountable disclosure
  - Compartmentalization and minimum necessary disclosure
  - Patients have the right to examine and correct information about themselves
  - Provides for release of “deidentified” data

# Timeline for EDI



Mandatory Compliance:
Claims Attachment Standards

No Later
Than 1Q2003
(0.7 Probability)

Final Rule: Claims Attachments

No Later Than
2Q2001
(0.7 Probability)

Claims Attachments
NPRM

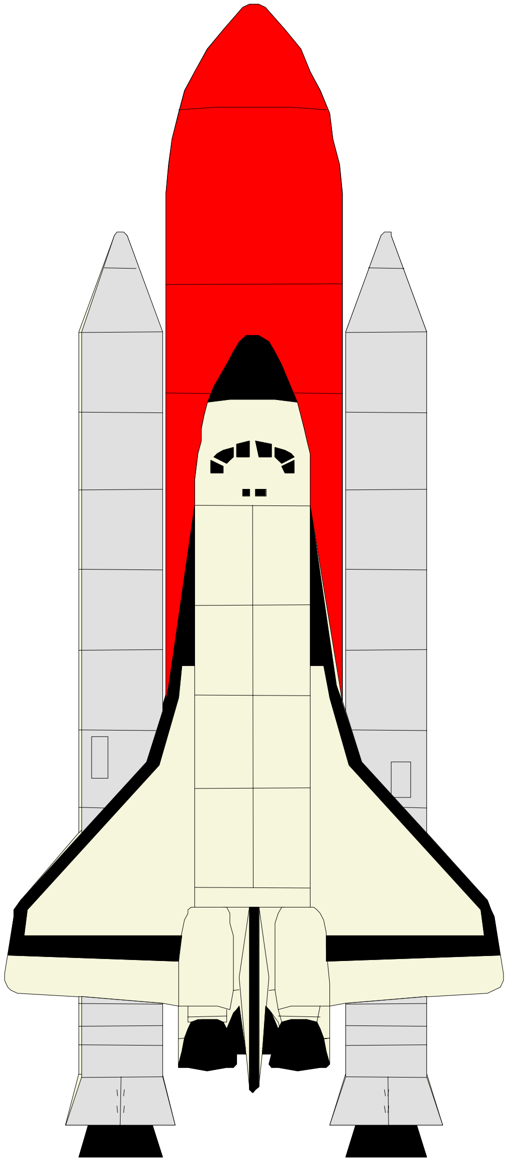
No Later Than 3Q2000
(0.7 Probability)

May 1998

NPRM on EDI Transactions and Code Sets

21 August 1996 HIPAA Enacted

# DHHS Standards for Electronic Transactions



## The Change Agent for e-Commerce in Healthcare

### ASC X12N Message Formats for:

- Claims/Encounters (837)
- Enrollment/Disenrollment (834)
- Eligibility (270/271)
- Payment and Remittance Advice (835)
- Premium Payments (811/820)
- Claim Status (276/277)
- Referral Certification and Authorization (278)
- Claims Attachments (expected: 275 + HL7 ORU)

### Ntnl Cncl for Prescription Drug Prgrms for:

- Retail Pharmacy Transactions

# Electronic Transactions and Code Sets

- Moving towards a “standard” standard
- Providers not required to submit electronically
- Use of clearinghouses
  - a fee from providers who can not produce a standard transaction
  - a fee from payers who can not process a standard transaction
  - the pass through “loophole”
  - potential requirements for internal changes remain-- data capture, code sets, identifiers
- Claims attachments (no NPRM yet)
  - not required of Providers
    - benefit = reduced people, paper & postage
  - “all or none” per claim
  - requires system integration or CPR

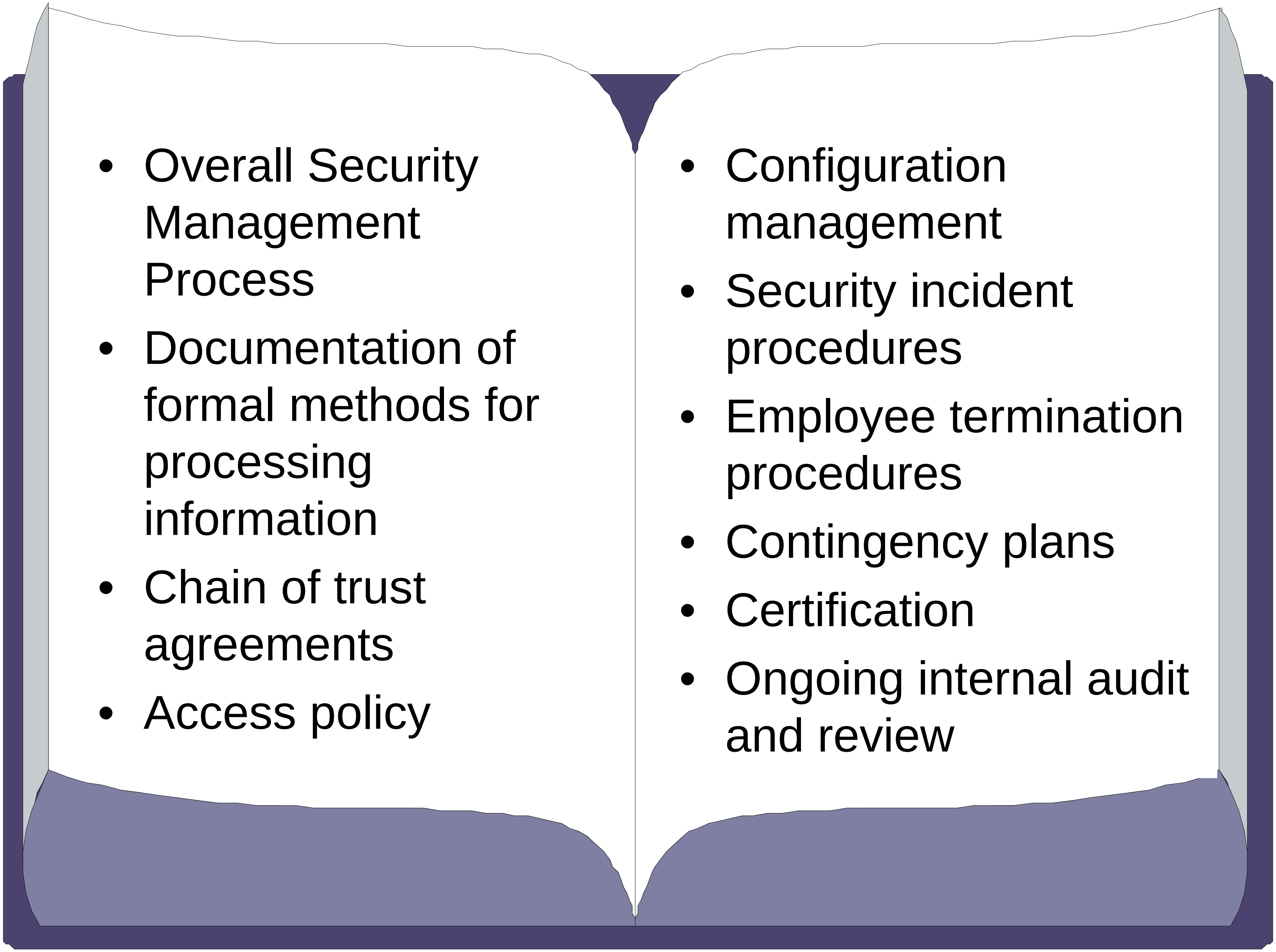
# EDI Standards: What to do Now

- Assess impact and business benefits
- Co-develop with other e-Health initiatives
- Do not wait for the final rule before getting started!
- Begin co-ordination with your vendors, clearinghouses, and trading partners
- Develop transaction implementation plans from IS and business perspective
- Identify your trading partners and develop testing criteria
- Use independently developed tools to test compliance with implementation guide

# Security and Electronic Signature Standards

- Administrative Procedures
- Physical Safeguards
- Technical Security Services - Information at Rest
- Technical Security Mechanisms - Information in Motion
- Electronic Signature

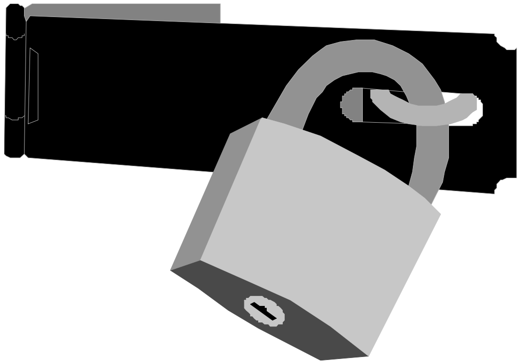
# Administrative Policies and Procedures



- Overall Security Management Process
- Documentation of formal methods for processing information
- Chain of trust agreements
- Access policy
- Configuration management
- Security incident procedures
- Employee termination procedures
- Contingency plans
- Certification
- Ongoing internal audit and review

# Physical Safeguards

- Assigned security responsibility
- Physical access control
- Media controls
- Work station use policy
- Secure workstation location



# Technical Security Services “Information at Rest”

- Entity authentication
- Entity access control
- Data authentication
- Patient authorization control
- Audit controls

# Technical Security Mechanisms "Information in Motion"

When Using Communications or Networks:

- Message Authentication & Integrity Control
- and One of the following:
  - Access Control
  - Encryption !! Mandatory for open networks !!

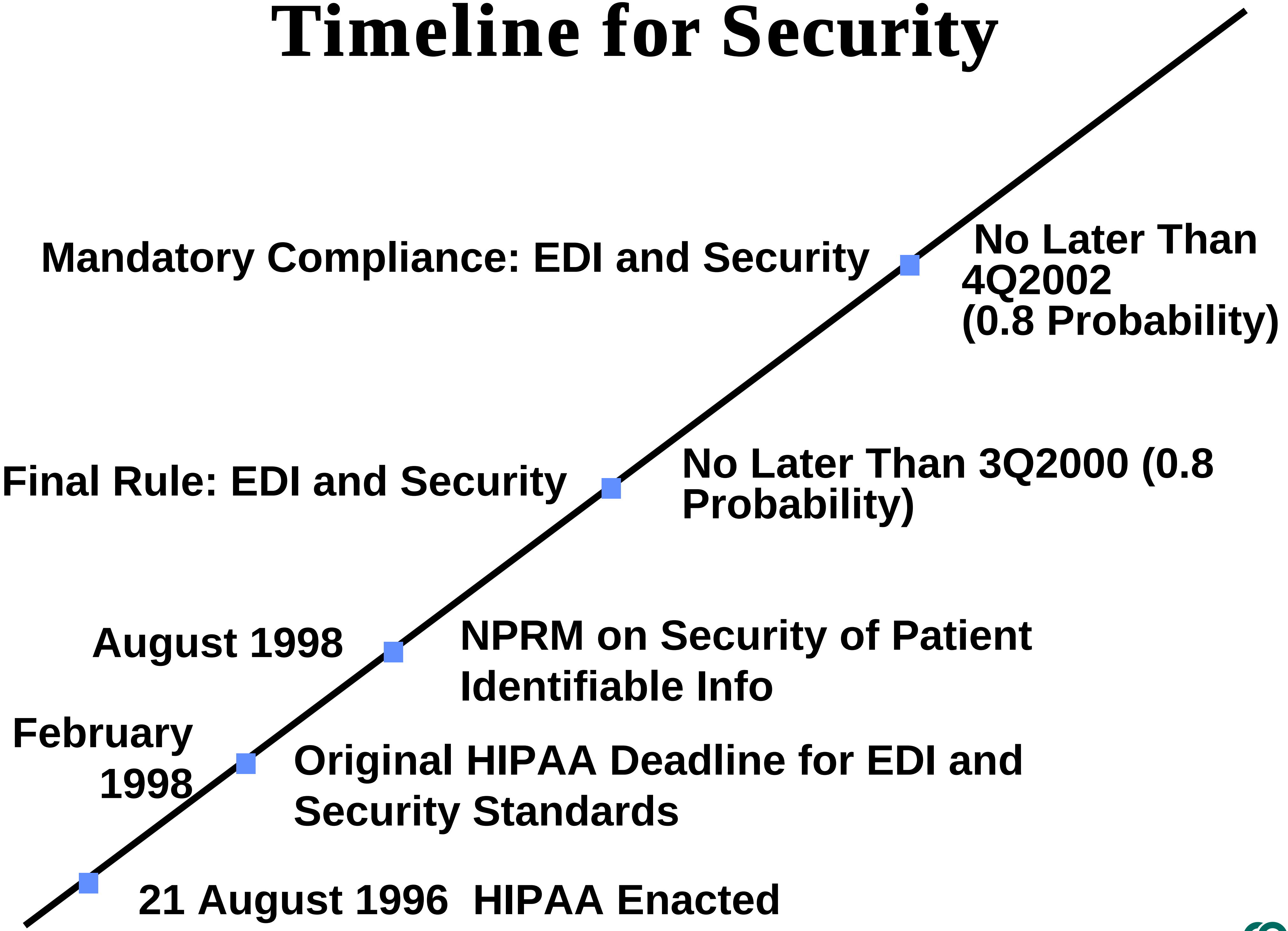
In Addition for All Use of Networks:

- Entity Authentication
- Event reporting and alarms
- Audit trail

# Electronic Signature Standard

- Applicability
  - No mandated use yet
  - If electronic signature used, it must adhere to standard
- A technological constraint
  - Must be “based on cryptographic methods”
- Required implementation features
  - Authentication of the signatory
  - Nonrepudiation
  - Message integrity
- Only commercial technology that can meet these requirements is Public Key Infrastructure (PKI)

# Timeline for Security



Mandatory Compliance: EDI and Security

No Later Than 4Q2002 (0.8 Probability)

Final Rule: EDI and Security

No Later Than 3Q2000 (0.8 Probability)

August 1998

NPRM on Security of Patient Identifiable Info

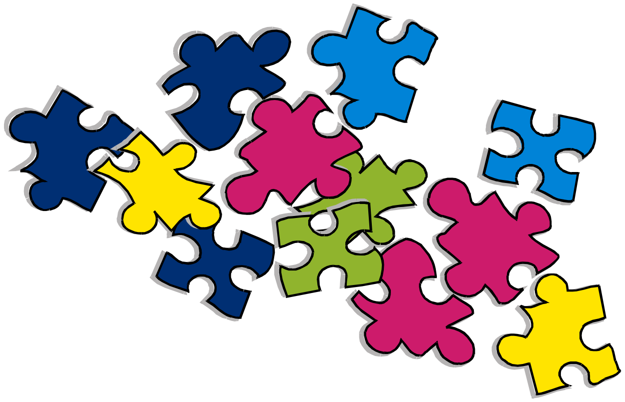
February 1998

Original HIPAA Deadline for EDI and Security Standards

21 August 1996 HIPAA Enacted

# AFEHCT & WEDI
# Internet Interoperability Pilot

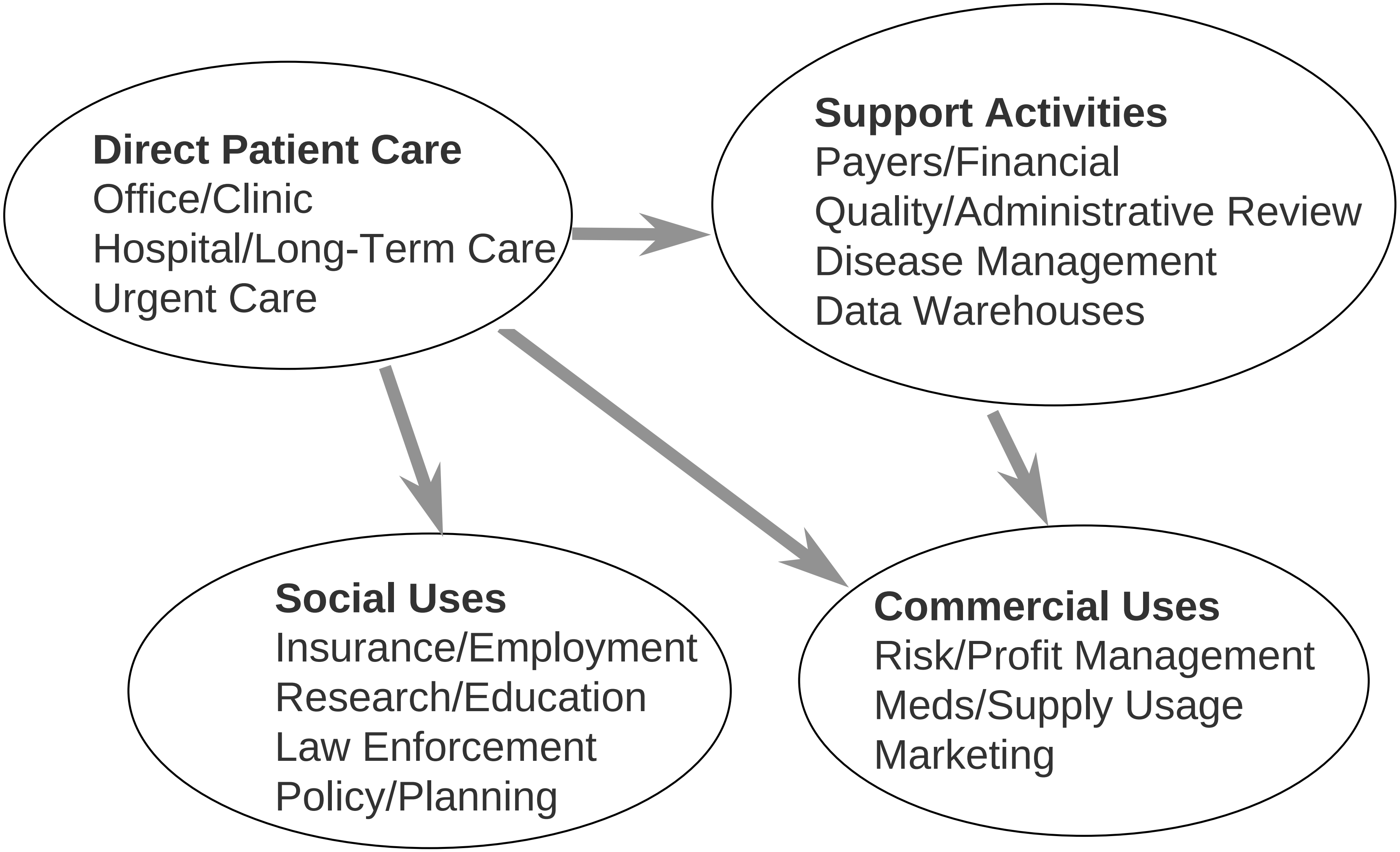
- Nominally about HCFA Medicare/Medicaid transaction
- In fact a Pilot of HIPAA Transactions and Code Sets
  - HHS watching for impact on final regulations
- 5 Working Groups
  - Batch EDI Transactions
  - Real-time EDI Transactions
  - E-mail transactions
  - Web Interfaces (browsers)
  - Security Interoperability (proposing a National Healthcare PKI)



# Security Standards: What To Do Now

- Hire a chief security officer (if revenues > $50 M)
- Train IS personnel in details of HIPAA security regs
- Train all personnel in their responsibilities and the personal and organizational consequences
- Develop a security gap analysis for infrastructure
- Pilot small PKI projects (secure E-mail, access)
- Quickly withdraw access for terminated employees
- Limit print/copy functions
- Program inactive workstation log-off

# Healthcare Data Flows/Vulnerabilities



**Direct Patient Care**
Office/Clinic
Hospital/Long-Term Care
Urgent Care

**Support Activities**
Payers/Financial
Quality/Administrative Review
Disease Management
Data Warehouses

**Social Uses**
Insurance/Employment
Research/Education
Law Enforcement
Policy/Planning

**Commercial Uses**
Risk/Profit Management
Meds/Supply Usage
Marketing

# Why Privacy?

- Longstanding concerns about misuse of patient’s data
- Fears exacerbated by increasing electronic storage and transmission
- “Something for everyone” in Congressional deliberations

# Principle of the NPRM

- Personal control over disclosure
  - Uncoerced, revocable authorization
  - Minimum disclosure
- Organizational compartmentalization.
- The right to examine and correct a person’s own information
- Mitigation
- Accountable disclosure
- “Deidentified” data
- Exceptions met with minimum disclosure
- Requirement for organizational diligence

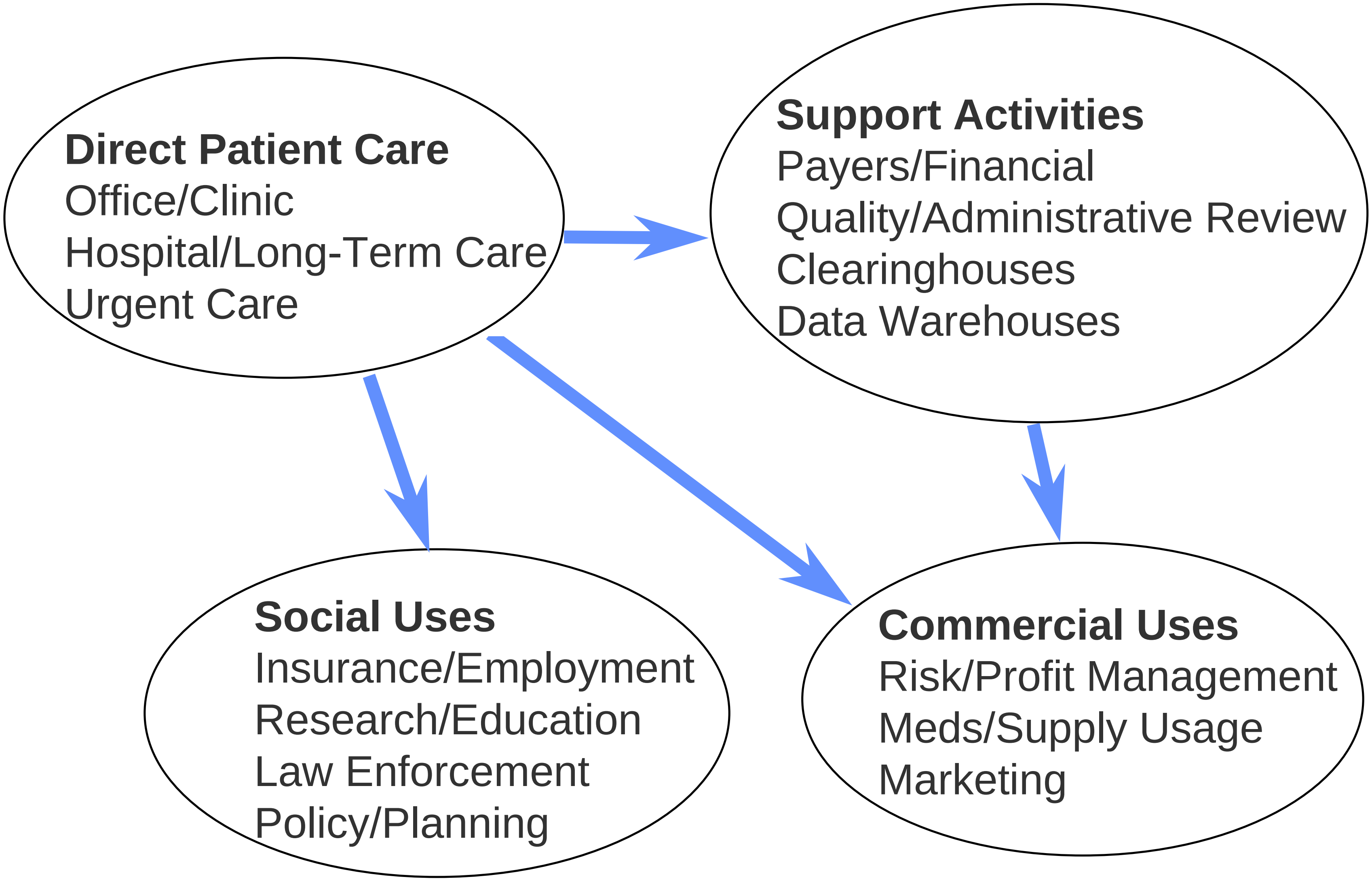
# Complicating Factors

- Covered entities and their business partners
- Electronic or paper form
- Ensuring uncoerced authorization
- Limits on deidentified data
- Specific requests not to disclose

# *Enforcement*

- No individual right of redress (at Federal level)
  - Third party beneficiary exception
- Limitations on civil fines
- Reasonable efforts and scalability
- Determining when state laws prevail

# Healthcare Data Flows / Vulnerabilities



**Direct Patient Care**
Office/Clinic
Hospital/Long-Term Care
Urgent Care

**Support Activities**
Payers/Financial
Quality/Administrative Review
Clearinghouses
Data Warehouses

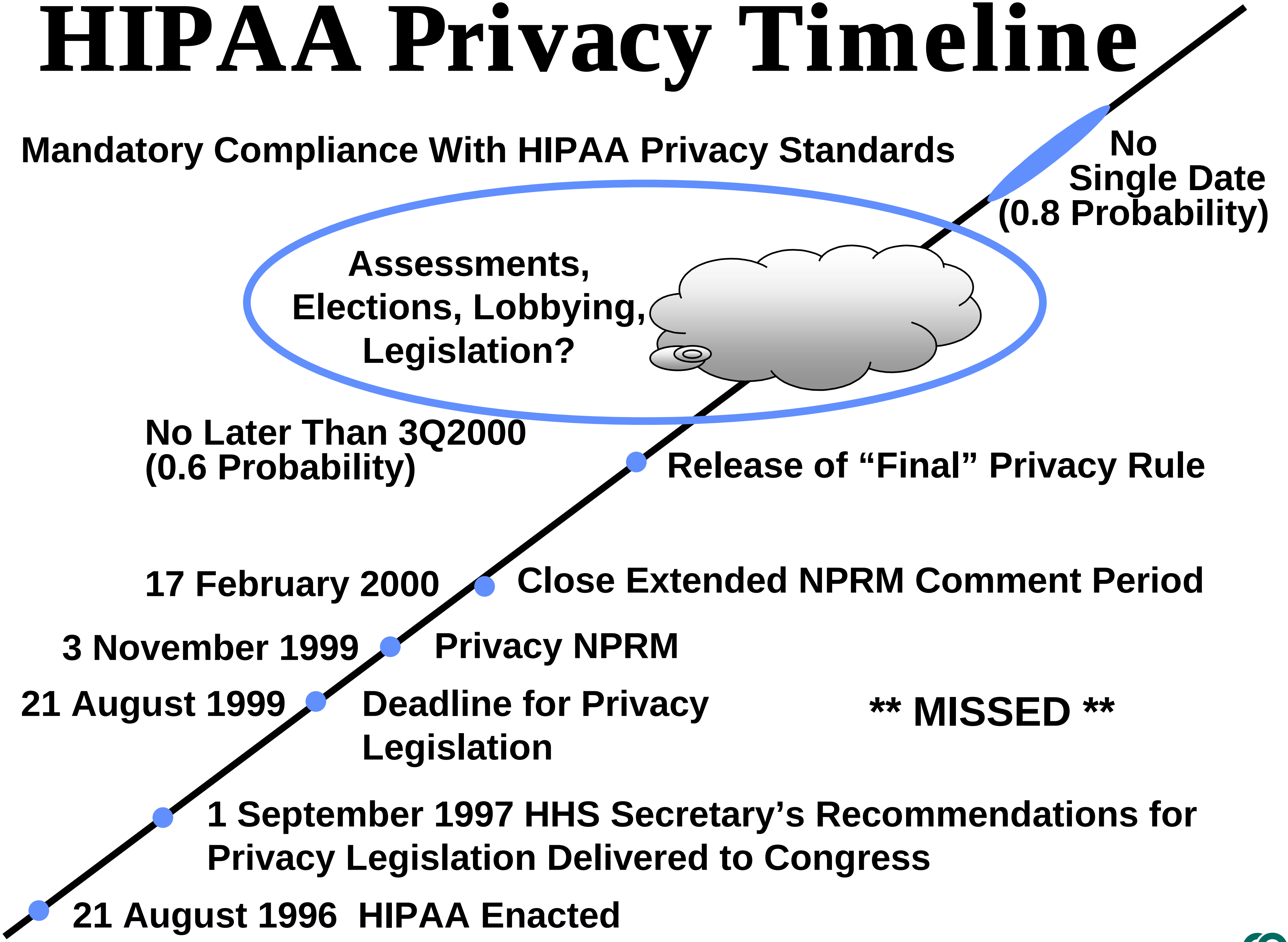
**Social Uses**
Insurance/Employment
Research/Education
Law Enforcement
Policy/Planning

**Commercial Uses**
Risk/Profit Management
Meds/Supply Usage
Marketing

# Seemingly Obvious Principles

- The federal government is practicing brinksmanship with Healthcare over cost containment
- The government will not break the back of healthcare over privacy costs
- To reduce the cost per year, spread the costs over more years

# HIPAA Privacy Timeline



Mandatory Compliance With HIPAA Privacy Standards

No
Single Date
(0.8 Probability)

Assessments,
Elections, Lobbying,
Legislation?

No Later Than 3Q2000
(0.6 Probability)

Release of “Final” Privacy Rule

17 February 2000 Close Extended NPRM Comment Period

3 November 1999 Privacy NPRM

21 August 1999 Deadline for Privacy Legislation

** MISSED **

1 September 1997 HHS Secretary’s Recommendations for Privacy Legislation Delivered to Congress

21 August 1996 HIPAA Enacted

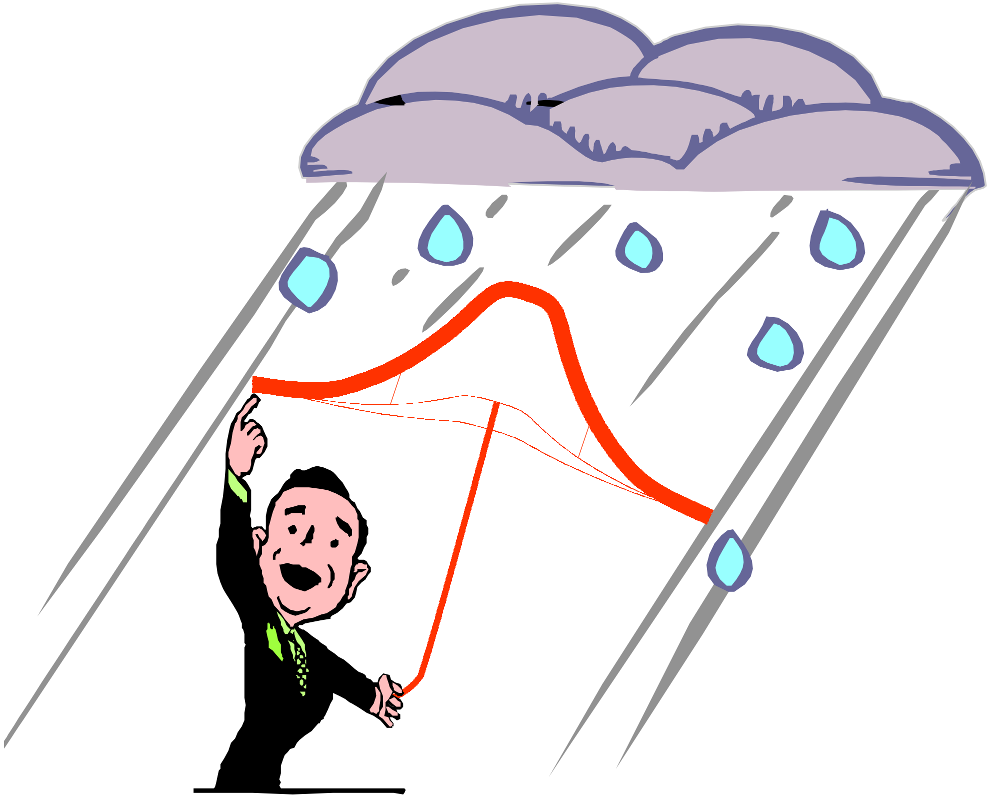
# What are the HIPAA provisions that will be in the Final Rule, survive the elections and have substantial, near-term impact on clients?

- Business benefit vs cost
- Cost vs. egregiousness
- Likely immediate concerns
  - organizational issues: policies, training, audit, procedures
  - trading partner agreements (unless the law is improved)
  - “reasonable” procedures to deal with correction and mitigation
- Likely longer term concerns
  - more precise auditing and mitigation
  - organizational compartmentalization

# At this uncertain moment, what measures can clients use as targets for privacy compliance?

- Avoid
  - malicious disclosure
  - non-responsiveness to patient concerns
  - systematic inability to comply with audit and mitigation requirements
- Standard of compliance is reasonable and scalable
- “Hide in the bell curve”

# HIPAA Strategies



**Security and Privacy**

**EDI**

Questions?